

C. Remarks

Based on the above amendments and remarks to follow, reconsideration of this application is respectfully requested.

In the third office action, claims 5 and 11 were rejected under 35 U.S.C. 112. Claims 5, 11, and 13 were rejected under 35 U.S.C. 101 and claim 16 was rejected under 35 USC 103(a). Further, claim 18 was objected to. Claims 1-4, 7-10, 22 and 23 were allowed. By this amendment, claims 5, 11, and 18 have been cancelled. Claims 13 and 16 have been amended to direct them to a practical application.

With respect to rejection of claim 5 and 11 under 35 U.S.C. 112, the Office Action states that the claims are indefinite. The office action further indicates that the claims result in hybrid claims as the dependent claims 5 and 11 recite "*a computer program product*" and their parent claims (Claim 1 and 7 respectively) recite "*a method*".

The Applicants have canceled claims 5 and 11 in the above amendment, in light of the rejection raised by the Examiner.

With respect to the rejection of claim 13 under 35 U.S.C. 101, the Office Action states that claim 13 recites the system without specific physical structures. Claim 13 has been amended by claiming the primality tester as a system. Further, claim 13 has been amended by incorporating the '*means for*' clause in the limitations a, b, and c to provide specific physical structures to the primality tester. The amendments are directed towards providing a concrete and tangible system for testing primality of a random number 'n', which can be used in encryption systems. The support for this recitation is found on page 7, lines 8-14.

With respect to the rejection of claim 16 under 35 U.S.C. 103(a), the Office Action

states that claim 16 has been anticipated by the abstract to Kaltofen et. al. (hereinafter referred to as "Kaltofen"). The Office Action also states that the claim 16 is unpatentable over the Background of the present invention combined with the teachings of Kaltofen, as claim 16 does not provide details about the "extension ring test" technique. Claim 16 has been amended by including various aspects of the primality tester. The amendments are directed towards providing the details of the system elements included within the primality tester which performs the extension ring test.

The applicants submit that the extension ring test as described in the present invention is substantially different from the ring test taught by Kaltofen. Kaltofen describes a modification of the *Goldswasser-Kilian-Atkin* primality test for testing the primality of the number 'n'. Kaltofen describes the use of Atkin's method which requires the notion of a "complex multiplication field" to compute an elliptic curve's order with an endomorphism ring. The endomorphism ring $End_F(E)$, consists of endomorphisms of E which fix F element wise. The endomorphism ring is isomorphic to a ring of integers of a given imaginary quadratic field $(Q\sqrt{-D})$. This field is said to be the complex multiplication field of E . Further, Kaltofen proposes use of *Watson class equations* along with quadratic field to test the primality of the number n . The Watson class equation is dependent on the equation:

$$w_{-D}(x) = x^h \prod_{k=1}^h \left(\frac{1}{x} - \sqrt{\alpha_k} \right).$$

The present invention is substantially different from the method explained by Kaltofen. The present invention as defined in the present claims is directed to an extension ring test to test the primality of a number n . The extension ring test is based on

the equation:

$$[g(x)]^n = g(x^n) \bmod(f(x), n)$$

The given equation is dependent on mod function based equations and polynomial function based equations. The primality of a number 'n' can be determined if the given equation holds true for the number n. The support for this recitation is found on page 8, lines 5-15 and page 10 lines 1-14 of the present application.

Hence, Kaltoven utilizes quadratic field as root of the Hilbert class equation to test primality of the number n. Moreover, the method is complex as it requires calculation of higher roots of a number. However, the present invention primarily utilizes mod function based equations to test the primality of a number 'n'. Consequently, the office action's conclusion that Kaltoven discloses a method for testing the primality of a number using the extension ring test is incorrect. The Applicant respectfully disagrees with the rejection of claim 16 and requests for the allowance of same.

The Office Action further states that a document by H. W. Lenstra, Jr., 'Primality testing with cyclotomic rings' is mentioned as a reference in one of the non-patent citations of the present invention, 'Primes is in P' by Agrawal et al, which was cited as an art of interest.

The Applicants respectfully bring to the USPTO's notice that the published paper by Agrawal, titled 'Primes is in P', has *two versions*. The first version *which is cited in the present invention* at the bottom of page 8 was made available on the internet on August 6, 2002 (a copy of which is attached hereto and is listed on the enclosed information disclosure form) and it does not refer to the document by H.W. Lenstra. The second version of the paper by Agrawal 'Primes is in P' was published with various revisions in

2004 (as cited in the present office action), and included a reference to 'Primality testing with cyclotomic rings' by H.W. Lenstra.

The document by Lenstra (a copy of which is attached hereto and is listed on the enclosed information disclosure form) provides an algorithm for testing the primality of a number using cyclotomic rings, which was based on the method explained in the first version of the paper 'Primes is in P' by Agrawal. Lenstra has described in his document that the method for testing primality testing using cyclotomic ring, is inspired from the extension ring test. Further, the first version of the paper "Primes is in P" has been cited as a reference in the document by Lenstra.

Further, the Applicant has attached hereto a copy, and listed on the enclosed information disclosure form, of an electronic mail between H.W. Lenstra and Dr. Manindra Agarwal (lead inventor of the present invention). The electronic mail is dated August 13, 2002 and makes clear that the study by H.W. Lenstra is based on the first version of paper 'Primes is in P'. The text of the email is as follows:

To Manindra Agrawal, Neeraj Kayal, Nitin Saxena,
 %Carl Pomerance, Dan Bernstein, R. Balasubramanian
 %
 % Leiden, August 13, 2002.
 %
 %Dear addressees,
 % Below a plain TeX file of an incomplete document that
 %contains an improvement of the test, for you to improve upon
 %further! Please understand that, apart from being incomplete,
 %it is in no way an official 'publication' or 'preprint', and
 %it may never become one. It is just to let you know where I
 %am standing at the moment, and I will greatly appreciate if
 %you reciprocate.
 % The only part below that I wrote with some care is
 %Section 1. The quantity to look out for if you want to
 %understand where my improvement comes from is u , which is
 %the index of the subgroup generated by p and n modulo r .
 %If u is large then the pigeonhole principle at the end of

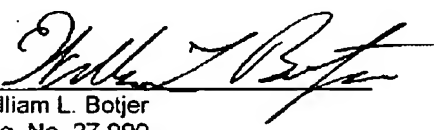
%the original proof can be improved. If u is small, then a
 %much more important improvement can be carried through, since
 %(roughly speaking) the group generated by the $X - a \pmod{((X^r - 1)/X - 1), p}$ becomes 'almost cyclic' (more
 %precisely: a product of u cyclic groups), which is an
 %obvious advantage. So no value of u is critical for the
 %original proof, and that is why introducing u leads to an
 %improvement. (In my write-up below, I followed Dan's advice
 %of not insisting upon units, so the group G got replaced by
 %a semigroup S .) Somewhat surprisingly, the choice of the
 %prime divisor p of n is now immaterial.
 % The later Sections are very sketchy only. I hope they
 %are correct, and that you can improve upon them.
 % I will be very interested in any comments you may have.
 % All the best,
 % Hendrik Lenstra

Accordingly, the time frame of the Lenstra paper is made clear.

It is respectfully submitted that the application is now in condition for allowance. If the Examiner has any questions regarding this matter, the Examiner is requested to telephone the applicants' attorney at the numbers listed below, prior to issuing an advisory action.

Dated: October 1, 2007

Respectfully Submitted,

By 
 William L. Botjer
 Reg. No. 27,990
 PO Box 478
 Center Moriches, NY 11934
 (212) 737-5728 (Tue-Thurs)
 (631) 874-4826 (Mon & Fri)
 (631) 834-0611 (cell if others busy)